

# Data Sharing Agreement

## 1. Overview

1.1 The following agreement between (1) The University of Reading (“**University**”) and (2) Reading University Students’ Union (“**RUSU**”) reflects the arrangements that they have agreed to put in place to facilitate the sharing of Personal Data relating to students studying at the University between the two as data controllers, and explains the purposes for which that information may be used.

1.2 In consideration of the mutual benefits in exchanging Information, and in further consideration of each party agreeing to pay to the other, on demand, the sum of £1, the parties agree to be bound by the terms in this data sharing agreement.

1.3 Capitalised words in this agreement will have the meanings set out in Schedule 1.

## 2. Purpose for data sharing and how students’ personal information will be used by RUSU

2.1 RUSU is a student body providing a range of services, facilities and personal development opportunities for students at the University to enable and supplement their academic studies. As a general rule, all students on a University of Reading course resulting in a qualification are members of RUSU and able to participate in the functioning of the union. However, in some cases, students studying outside the UK may not be able to participate in the functioning of a union due to the law of the country in which they are studying.

2.2 RUSU requires access to certain personal information relating to students at the University to ensure that all eligible students are informed of, and able to fully participate in the services and opportunities available via the union.

2.3 The sharing of the Information is intended to support the following objectives of RUSU:

- to support the efficient and effective communication of RUSU services to all students at the University;
- to support the efficient and effective engagement of all eligible students in the democratic functions of RUSU
- to enable effective management and planning of RUSU services and facilities by receiving comprehensive demographic information

2.4 In particular, RUSU will only use the Information for the following purposes:

- Administration of elections
- Administration of RUSU clubs, societies, Junior Common Rooms’ (JCRs) and their memberships
- Generation of demographic reports
- Verification of student’s identity and eligibility
- Administration of ticket sales

- To allow email communication between RUSU and its members
- To allow email communication between its Clubs & Societies members where no emails are visible to the sender (Sender; Committee members of the Club/Society)

### 3. Information to be shared

3.1 The University will provide RUSU with the following student information from RISIS: mode of attendance; student code (Reading ID number); first name; middle name(s); surname; date of birth; sex; personal email address (until university one has been activated); university email address; Placement (whether a student is on placement or not); Erasmus indicator; Mature Student Indicator; Distance learner indicator; nationality; country of domicile; Location; Study Site; Home or Overseas status for fee payments; course code; course name; enrolment status; Student Type (Full time, part time), Mode of Study (i.e. UG, PG or other types); faculty; school; department; year of study, expected end of study date (or finalist flag), and where relevant, hall of residence.

3.2 No Sensitive Personal Data will be transferred between RUSU and the University.

3.3 The University will only provide Information for students on a University of Reading course resulting in a qualification. Information relating to the following students shall be excluded:

- Students who have left the University, withdrawn or deceased
- University of Reading Malaysia students
- College of Estate Management students
- Students on short courses (less than four weeks)
- Students studying outside the UK, where the University believes that that national laws of the relevant country (i.e. the country in which the student is studying a University of Reading course) do not permit its citizens to be a member of a union.
- any individual student who has indicated to the University that they do not want their data provided to RUSU (including those that wish to be excluded temporarily, whilst they wait for a university email address, because they do not wish their personal email address to be passed to RUSU)

3.4 The University and RUSU have jointly agreed that sharing the Information in accordance with this agreement for the Purposes is permitted under the Act, and will be fair and lawful on the basis that the following conditions set out in Schedule 2 of the Act are satisfied:

- the condition set out in paragraph 1 of Schedule 2 of the Act - that the individual data subject has consented to the transfer which is clearly identified in the fair processing notices given by the University to individual students;
- the condition set out in paragraph 2(a) of Schedule 2 of the Act, - that the processing is necessary for the performance of a contract between the student and the University;
- the condition set out in paragraph 6 of the Act - that the processing is necessary for the purpose of legitimate interests pursued by both the University and RUSU, which is the promotion of student welfare and active engagement by students in a function

and range of activities offered by RUSU to facilitate their education and development. The parties are satisfied that processing the Information as set out in this agreement will not prejudice the rights, freedoms or interests of individual data subjects

3.5 RUSU acknowledges that this is not a licence for unrestricted access to the Information, and that as the data controller of the Information it will be responsible for ensuring that all such Information is used and managed in accordance with the fair processing notices given to individual students and the Act.

#### **4. How to ensure that Information is used in accordance with the Data Protection Principles**

4.1 The Information will be provided via regular secure, encrypted electronic transfer in accordance with the University's encryption policies which as at the date of this agreement can be found at <http://www.reading.ac.uk/web/FILES/imps/Encryption-Policy-CURRENT.pdf>, but may be amended from time to time. The transfer will ensure that RUSU, or any data processor processing on behalf of RUSU, will hold up-to-date Information at that time and enable RUSU to take steps to prevent further Processing of any Information where it is advised by the University that an individual student has opted out of the data sharing agreement.

4.2 In order to give the University assurances that RUSU will handle all such Information appropriately, and in accordance with the Data Protection Policies, RUSU will:

- only process Information to deliver the Purposes set out above,
- limit access to the Information to those of its officers, staff, agents and sub-contractors who need to know and access the Information to deliver the Purposes;
- ensure that those of its officers, staff, agents and sub-contractors accessing the Information receive regular training on data handling good practice, and in particular, that they undertake and pass the University's online data protection and information security modules ([www.reading.ac.uk/data-protection-training](http://www.reading.ac.uk/data-protection-training))([www.reading.ac.uk/information-security-training](http://www.reading.ac.uk/information-security-training))
- ensure that those of its officers, staff, agents and sub-contractors accessing the Information are aware of the confidential and sensitive nature of the Information;
- ensure that there is a written agreement with any third party engaged to Process the Information on behalf of RUSU that contains provisions equivalent to those set out in this data sharing agreement, and the data processing clauses in Schedule 2 in particular. The University reserves the right to withhold transfers of data where it reasonably considers that any arrangements with a third party do not satisfy this requirement.

4.3 In order to give RUSU assurances, the University will take reasonable steps to ensure that the Information enclosed in any data transfer is accurate at the time of the transfer, and that it will take reasonable steps to ensure the quality of the Information in accordance with the University's own data protection policies and procedures from time to time.

4.4 The University will take reasonable steps to ensure that any Personal Data relating to an individual student who notifies the University that they do not wish their information to be shared with RUSU is excluded from the Information, and RUSU will be responsible for ensuring that it operates appropriate "opt out" arrangements. In the event of any conflict between data held by RUSU and Information shared by the University, RUSU will work

cooperatively with the University to reconcile the difference as soon as reasonably practical. However, it will be RUSU's responsibility (and any sub-contractors) to check the Information provided by the University against its own opt-out records to ensure any opt outs it receives directly from students are flagged by it onto its own records of the Information. In particular, RUSU acknowledges that it may obtain specific opt-outs from students for some of RUSU's services but not others and the University data feed would only be able to reflect blanket opt-outs.

## **5. Data Security Requirements**

5.1 RUSU will maintain appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of Information; and against accidental loss or destruction of, or damage to, the Information shared by the University, and in particular will comply with the following information security arrangements:

- Transfers of the Information will only be shared in accordance with the encryption policy at <http://www.reading.ac.uk/web/FILES/imps/Encryption-Policy-CURRENT.pdf>;
- Information will be kept confidential, and the University and RUSU will each ensure that their officers, staff and representatives are appropriately trained in handling personal data;
- RUSU will ensure that its offices, equipment and IT systems are appropriately secured with both physical and technical security measures to prevent access to the equipment and the data stored thereon. Such physical security measures include:
  - ensuring IT equipment, including portable equipment is kept in lockable areas;
  - not leaving portable equipment containing the Information unattended;
  - ensuring that staff use appropriate secure passwords for logging into systems or databases containing the Information

such technical security measures include:

- ensuring that all IT equipment is protected by antivirus software, firewalls, passwords and suitable encryption devices;
- only transferring data on encrypted USB or other portable devices;
- limiting access to relevant databases and systems to those of its officers, staff agents and sub-contractors who need to have access to the Information, and ensuring that passwords are changed and updated regularly to prevent inappropriate access when individuals are no longer engaged with RUSU.
- Information that is no longer needed is securely, and permanently deleted, and in particular RUSU will ensure that it adheres to the University's records retention policies for student personal information.

## **6. Retention and Deletion of Information**

As a data controller, RUSU is responsible for ensuring that it operates an appropriate data retention policy, and will ensure that Information is routinely deleted when it is no longer required in accordance with the requirements of the third data protection principle (that personal data shall be relevant to the purpose for which it is processed) and the fifth data protection principle 5 (that personal data shall not be kept for longer than is necessary for the specific purpose for which it is processed).

When the Information is no longer required to achieve one or more of the Purposes, or if this agreement is terminated, RUSU will either return all copies of the Information that is

has made, or ensure that all such copies are securely destroyed. Where Information is temporarily not required (but a copy is required to be retained in accordance with the University's data retention policy or good information management practice) RUSU will ensure that such copies are held in a secure storage facility, separate from its active databases until it is either required or destroyed.

## **7. Fairness of Processing and rights to Opt Out**

7.1 The University has considered the need to ensure fairness to the individual students, and will ensure that all registering students are given appropriate information about the data sharing, including a right to opt out of the sharing for the Purposes set out in this data sharing agreement. This will be communicated by way of the University's fair processing notice (at <http://www.reading.ac.uk/internal/student/OnlineStudentHandbook/osh-dataprotection.aspx>) and via other communications with students. RUSU will ensure that its use of the Information is consistent with the Purpose and the University's fair processing notice, and in particular that it will not use or provide the Information to any third party without the express consent of the individual(s) concerned, except

- where RUSU has obtained the written or minuted permission from Chair of the Student Experience Committee;
- where information is passed to an agent or sub-contractor processing on behalf of RUSU for the purpose of operating the website or other activity on behalf of RUSU and only where there is an appropriate written agreement as set out in paragraph 4.2 above.

7.2 RUSU will not without the express and informed permission of the individual student use the Information supplied by the University for any marketing services or activities other than for RUSU's own activities or products or services that directly and genuinely benefit students, and only where the students are given an easy to use option in each mailing to opt out of future mailings. Where RUSU intends to issue any bulk emails, it will notify the University's IT Services sufficiently in advance and take appropriate action of any reasonable request to delay or reschedule such bulk emails.

7.3 RUSU shall maintain a readily accessible and easy-to-use mechanism for students to opt out of having their personal information being processed by RUSU at any time.

## **8. Complaints and Subject Access**

8.1 The University and RUSU will jointly work to address any complaint from an individual regarding the processing of his or her Personal Data under this data sharing agreement.

8.2 The University and RUSU will each co-operate in relation to a request from the other to respond to a subject access request relating to the Information. Primary responsibility for responding to any subject access request will remain with the party to whom the subject access request is addressed.

## **9. Review and publication**

9.1 This agreement is to be reviewed annually to ensure that the Purposes remain valid and the Information and procedures set out in this data sharing agreement continue to reflect the requirements of the Act, and the requirement to ensure fairness of individual students.

9.2 RUSU agrees that the University may conduct an audit of RUSU or any Data Processor it appoints to support its activities, to ensure compliance with the requirements of this data sharing agreement.

9.3 In the event of any disagreement as to the implementation, or interpretation of the requirements of this data sharing agreement, the issue will be initially discussed between the Data Protection Officer on behalf of the University and Chief Executive of RUSU. In the event that the issue cannot be resolved within 10 days where an actual or imminent security incident is involved or 30 days for any other issue, the issue will be escalated to the Vice Chancellor of the University for resolution, and the decision of the Vice Chancellor will be binding on both the University and RUSU.

9.4 RUSU acknowledge that the University may suspend and/or terminate the provision of further data at any time, with or without notice, where the University acting reasonably considers that the safeguards for the Information are not adequate or adequately implemented to protect the rights of individual students.

9.5 This agreement will be published on the University and RUSU websites and linked from the University's fair processing notice:  
<http://www.reading.ac.uk/internal/student/OnlineStudentHandbook/osh-dataprotection.aspx>

9.6 Nothing in this data sharing agreement will limit or restrict either the University or RUSU's obligation to ensure compliance with the Act in relation to data where they are the Data Controller.

---

David Savage  
Chief Operating Officer  
The University of Reading

---

Date

---

Richard J. Silcock  
Chief Executive  
Reading University Students' Union

---

Date

## Schedule 1: Defined Terms

- **Information:** means the personal data relating to students studying at the University shared by the University with RUSU under this data sharing agreement, including the data fields set out in paragraph 3.1.
- **Purpose:** means the objectives for sharing the Information described in paragraphs 2.2, 2.3 and 2.4.
- **Act:** means the Data Protection Act 1998, and any relevant guidance or implementing regulations.
- **Data Subject, Data Controller, Data Processor, Processing and Personal Data** have the meaning set out in the Act.

## Schedule 2: Data Processing Terms

### Standard Data Processing Provisions for third party handling of Personal Data provided by the University to RUSU.

In these standard terms:

“**RUSU**” means the Reading University Students Union;

“**Supplier**” means the third party supplier of services that includes the possession, storage, collection, maintenance, updating or any other use of personal data.

“**Services**” means the services to be provided by the Supplier to RUSU

“**Personal Data**” means personal data (as defined in the Data Protection Act 1998) relating to students at Reading University submitted or made available to the Supplier in connection with the provision of the Services

“**Data Controller**” “**Data Processor**”, “**Processing**” have the meanings set out in the Data Protection Act 1998.

1.1 The parties agree that RUSU is the Data Controller and that the Supplier is the Data Processor in respect of Personal Data processed in the provision of the Services.

1.2 The Supplier will process the Personal Data on behalf of RUSU only for the purposes of performing the Services and only in accordance with instructions contained in these clauses or received from an authorised RUSU staff member from time to time;

1.3 In order to protect the confidentiality and integrity of the Personal Data, the Supplier will implement appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, including but not limited to:

- ensuring IT equipment, including portable equipment is kept in lockable areas;
- not leaving portable equipment containing the Information unattended;
- ensuring that staff use appropriate secure passwords for logging into systems or databases containing the Information;
- ensuring that all IT equipment is protected by antivirus software, firewalls, passwords and suitable encryption devices;
- only transferring data on encrypted USB or other portable devices;
- limiting access to relevant databases and systems to those of its officers, staff agents and sub-contractors who need to have access to the Information, and ensuring that passwords are changed and updated regularly to prevent inappropriate access when individuals are no longer engaged with RUSU;
- conducting regular threat assessment or penetration testing on systems

and will provide RUSU with a written description of any such technical and organisational measures from time to time on request.

1.4 The Supplier will ensure that only those staff, agents or contractors who need to have access to the Personal Data to deliver the Services do so, and will take reasonable steps to ensure the reliability of such individuals, and ensure that they are informed of, and understand the confidential nature of, the Personal Data, and the obligations set out in these clauses.

1.5 The Supplier shall not

- transfer any Personal Data to any third party, including any agent or sub-contractor, whether or not in connection with the provision of the Services without the prior written consent of an authorised RUSU staff member; or
- publish, disclose or divulge any Personal Data to any third party, including any individual subject of the Personal Data without written authorisation from RUSU

1.6 The Supplier will only modify, amend or alter the content of the Personal Data, in accordance with the scope of the Services, or any written instruction from RUSU to update, cleanse, amend or use the Personal Data.

1.7 The Supplier acknowledges that the Personal Data is confidential information, and will be treated with the same degree of care and confidentiality as the Supplier's own confidential information.

1.8 The Supplier will ensure that it implements appropriate and permanent data deletion in accordance with RUSU's policies or any specific request.

1.9 If any request for access to any Personal Data or complaint relating to the use of Personal Data is received by the Supplier, the Supplier will pass such request to RUSU and co-operate with RUSU in investigating and managing any such request or complaint but will not respond to the individual unless specifically authorised by RUSU.

1.10 RUSU may conduct or procure an inspection or audit of the Supplier's activities and data protection measures to ensure that the Supplier and its agents are fully compliant with these obligations. The Supplier will implement any measures reasonably directed by RUSU to ensure compliance with these clauses.

1.11 The Supplier acknowledges that it may not transfer Personal Data outside the European Economic Area without the prior written consent of RUSU, and that RUSU may require the Supplier to comply with and/or implement additional procedures, measures or contractual provisions to ensure the adequacy of protections of such Personal Data.

1.12 Each party will promptly notify the other if it becomes aware of any security breach, including any inappropriate use of or disclosure of Personal Data, and the Supplier will cooperate with RUSU to investigate the cause of, and mitigate the effects of any such security breach.

1.13 The Supplier will indemnify RUSU and keep RUSU indemnified against all losses, damages, costs or expenses and other liabilities (including legal fees) incurred by, awarded against or agreed to be paid by RUSU arising from any breach of the Supplier's obligations under these clauses.

1.14 RUSU may terminate the agreement with the Supplier immediately on notice, in the event of any material or persistent breach of these data processing provisions. On termination, the Supplier will immediately discontinue any further processing of Personal Data, and will at the request of RUSU return and/or permanently, and securely delete any and all copies of the Personal Data within the possession or control of the Supplier.